Automatização de Técnicas para Teste de Invasão

Agenda de Hoje

-Conceitos (Automatização, Teste de Invasão)

-Estudo de Caso
---Conhecimento e Aprendizagem
---Melhorando o que usamos hoje

-Ferramentas de Automatização
---Enumeração
---Teste de Invasão

Conceitos - Automatização

Automatização

Tem como objetivo principal fazer com que os **métodos** de trabalho sejam mais **fáceis**, **sem** a necessidade de **execução manual**, abrindo caminho **para uma atuação automática**.

Conceitos - Automatização

Automatizar é somente rodar ferramenta?

Automatização realmente e eficiente?

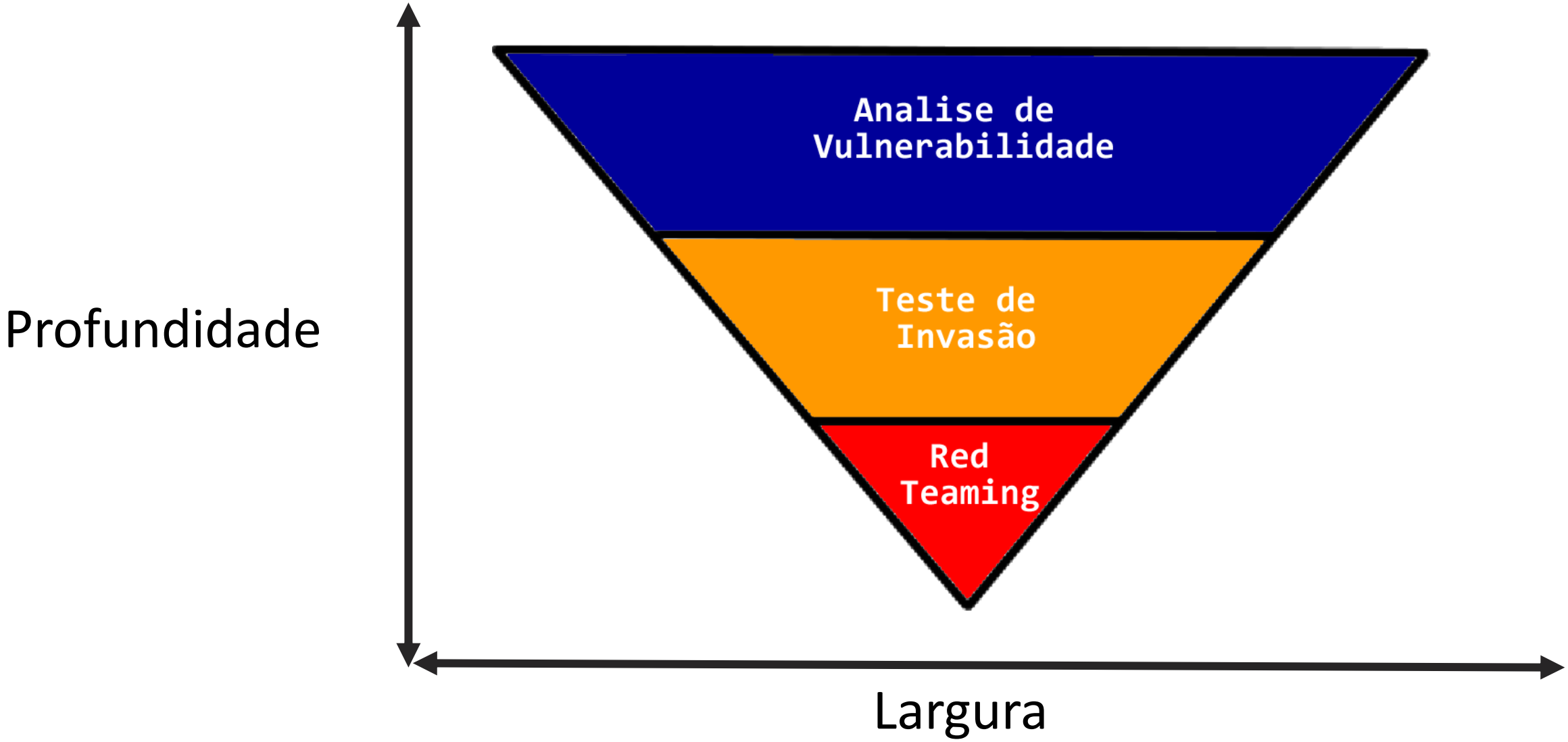
Se eu não conheço como eu automatizo?

Conceitos - Teste de invasão

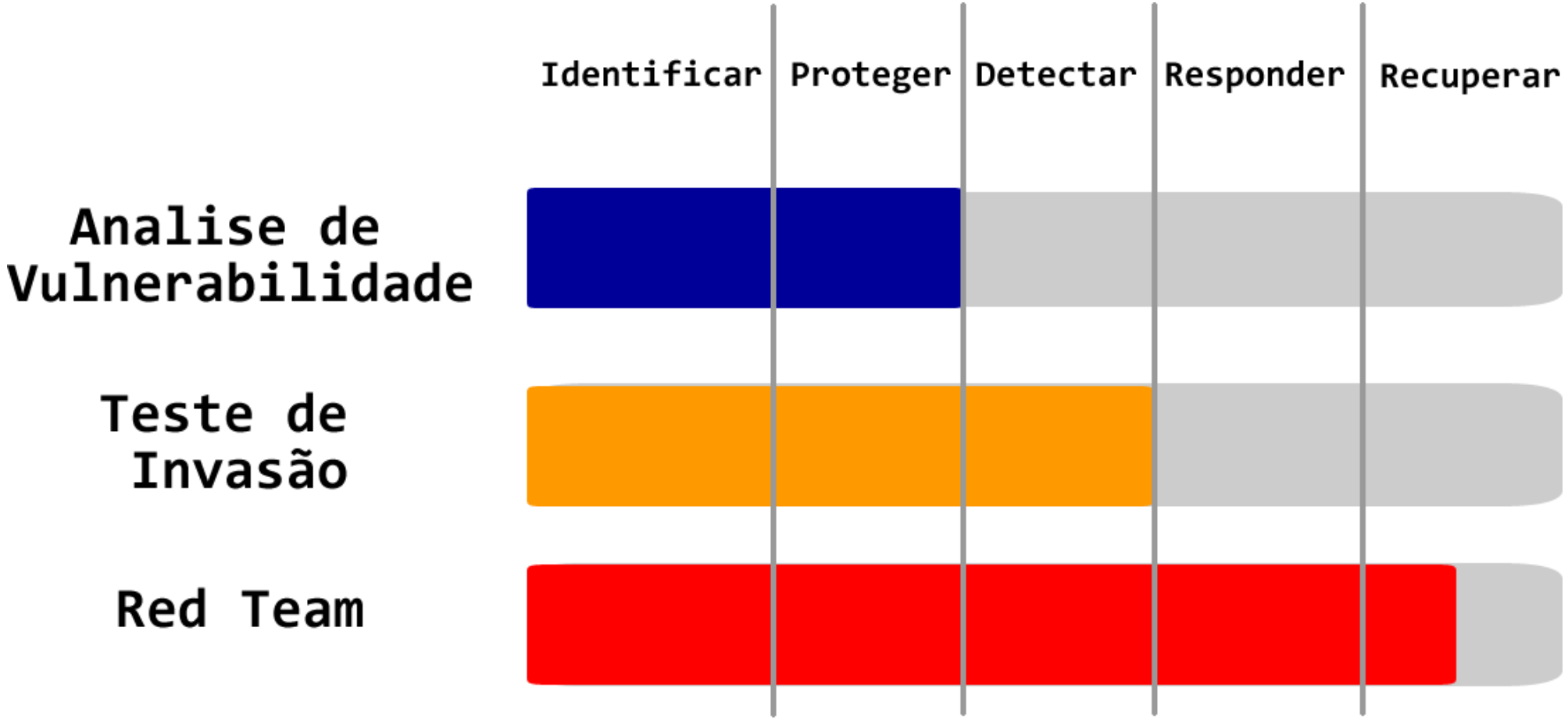
De acordo com a Publicação do **NIST 800-53** (Rev. 4),
o Teste de Invasão é definido como:

"... um **tipo** especializado **de avaliação** realizada em sistemas de informação ou em indivíduos componentes do sistema **para identificar vulnerabilidades** que poderiam ser exploradas por adversários ... "

Conceitos


Profundidade
Analise de Vulnerabilidade
Teste de Invasão
Red Teaming
Largura

Conceitos


Identificar
Proteger
Detectar
Responder
Recuperar
Analise de Vulnerabilidade
Teste de Invasão
Red Team

Conceitos

Equipes de Red Team, raramente executam ferramentas de analise de vulnerabilidades. **(Joe Vest)**

- Qual e sua atuação? (Pentest ou Red Team)
- Escopos Diferentes?

Então um Red Team não automatiza suas atividades?

Conceitos - Aprofundamento

Quais são essas atividades?

- Reconhecimento
- Enumeração
- Analise de Vulnerabilidade
- Exploração
- Pôs Exploração
- Relatório

O que iremos Automatizar?

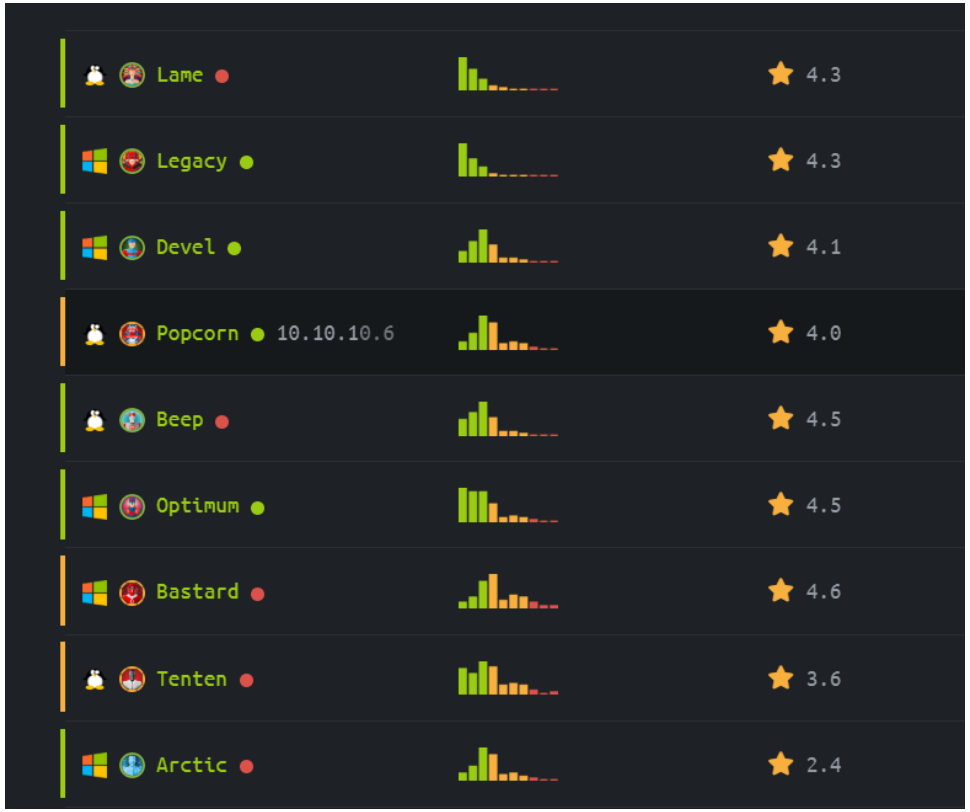
Estudo de Caso

Hack The Box

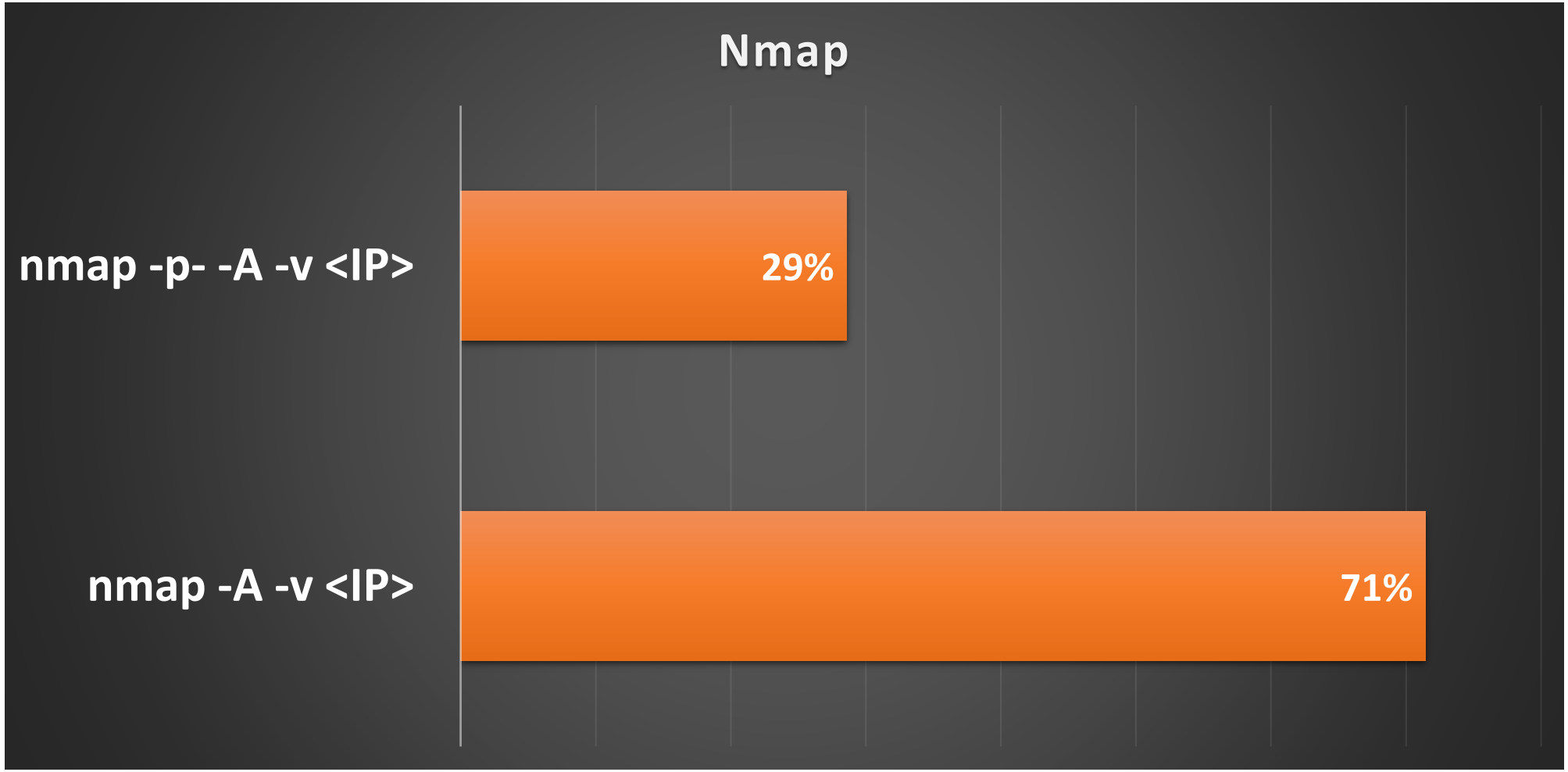
Hack The Box

Escopo da Pesquisa:

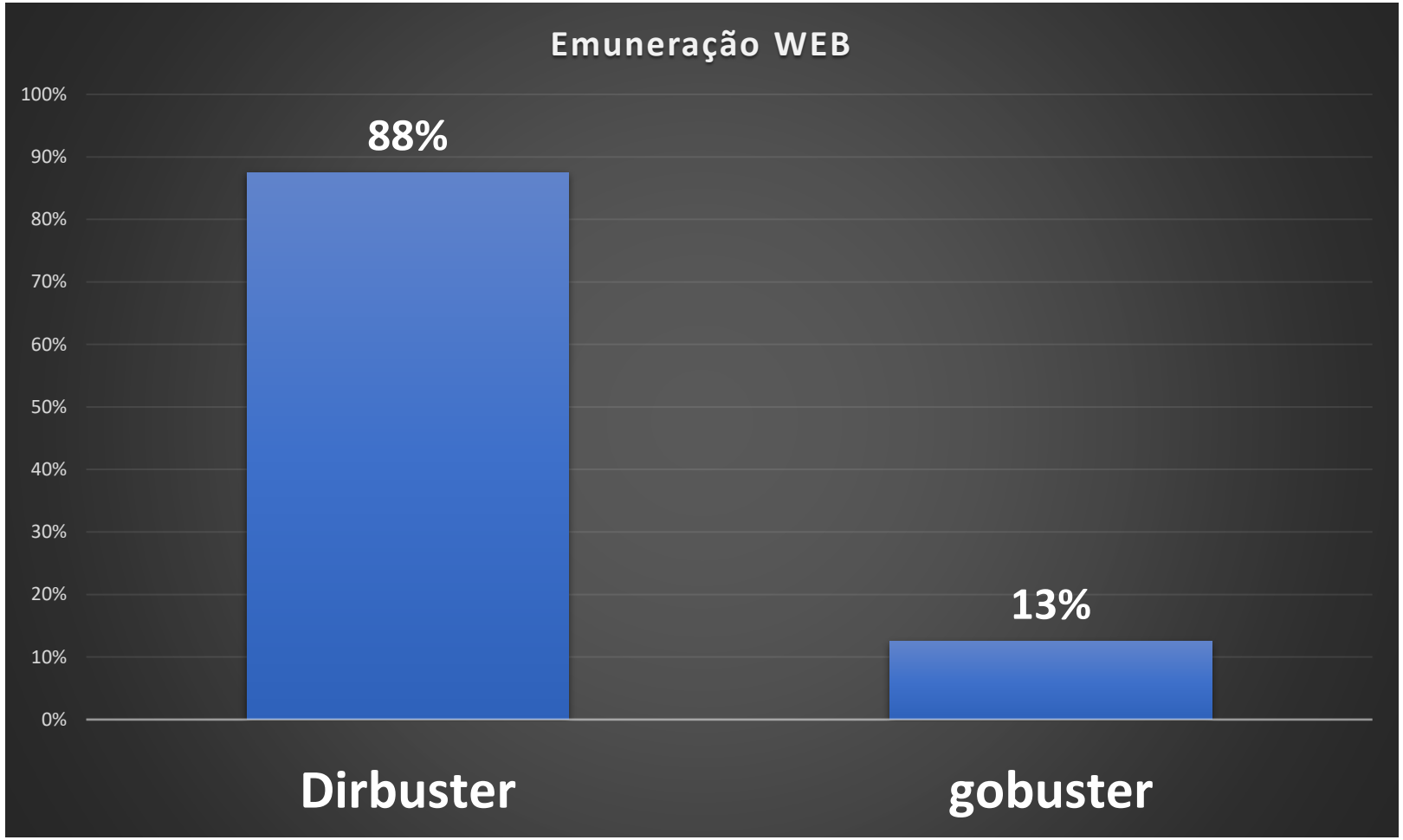
- 42 Maquinas
- Nível Fácil
- 2017 a 2020
- Somente Maquinas aposentadas



Hack The Box – Enumeração Inicial

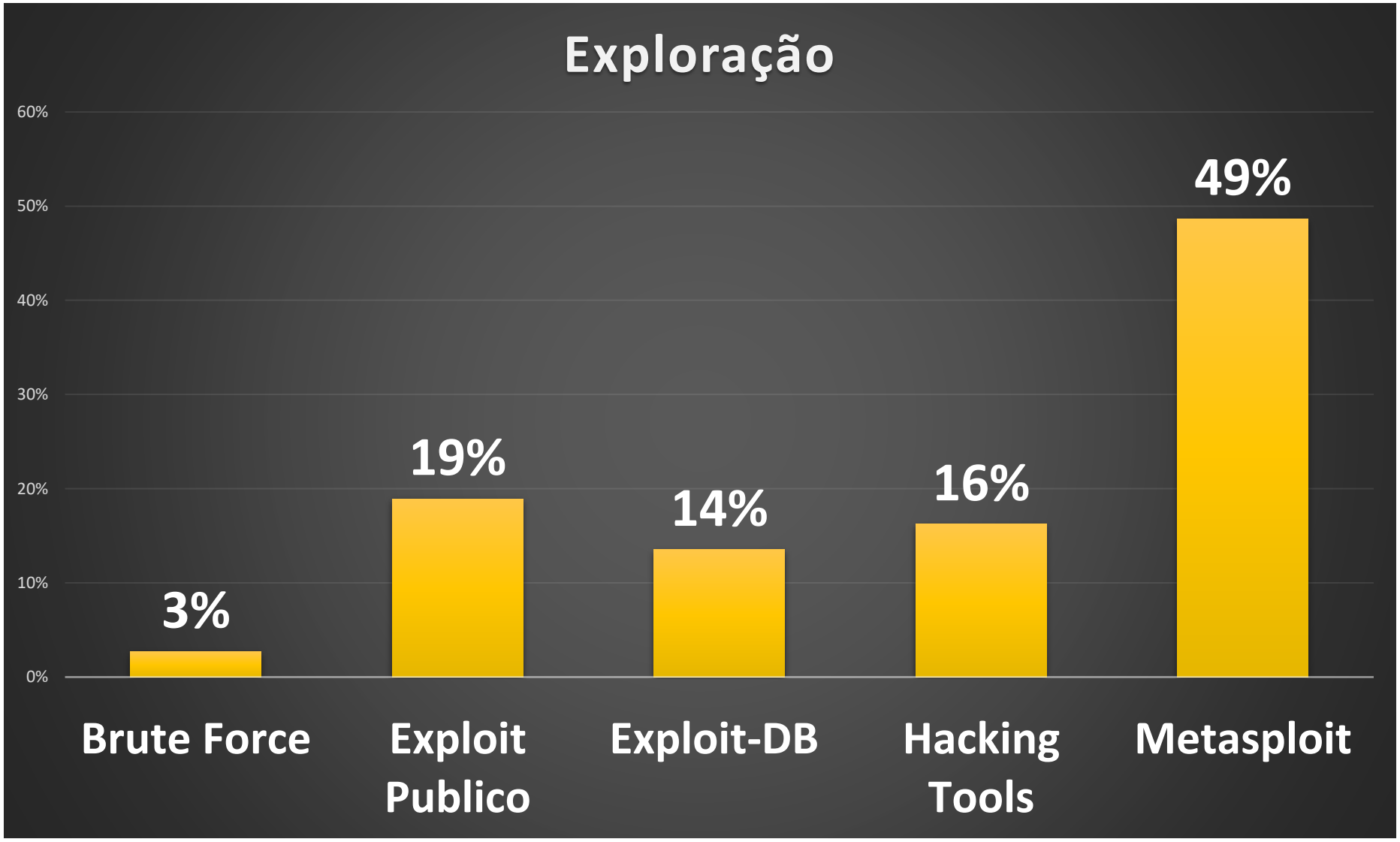


Hack The Box – Enumeração WEB

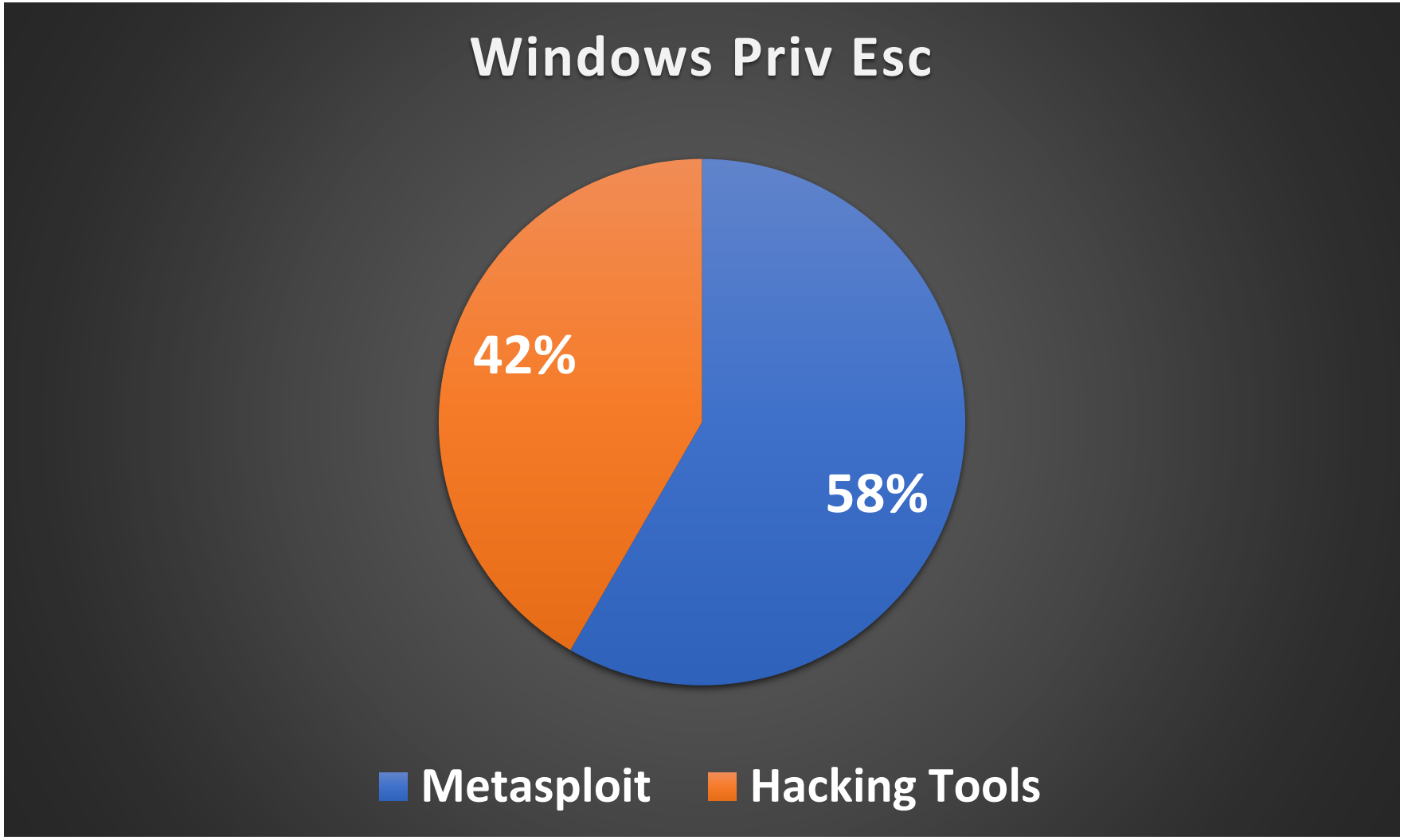


***Considerando apenas a amostra de maquinas que contem servidor WEB**

Hack The Box – Exploração

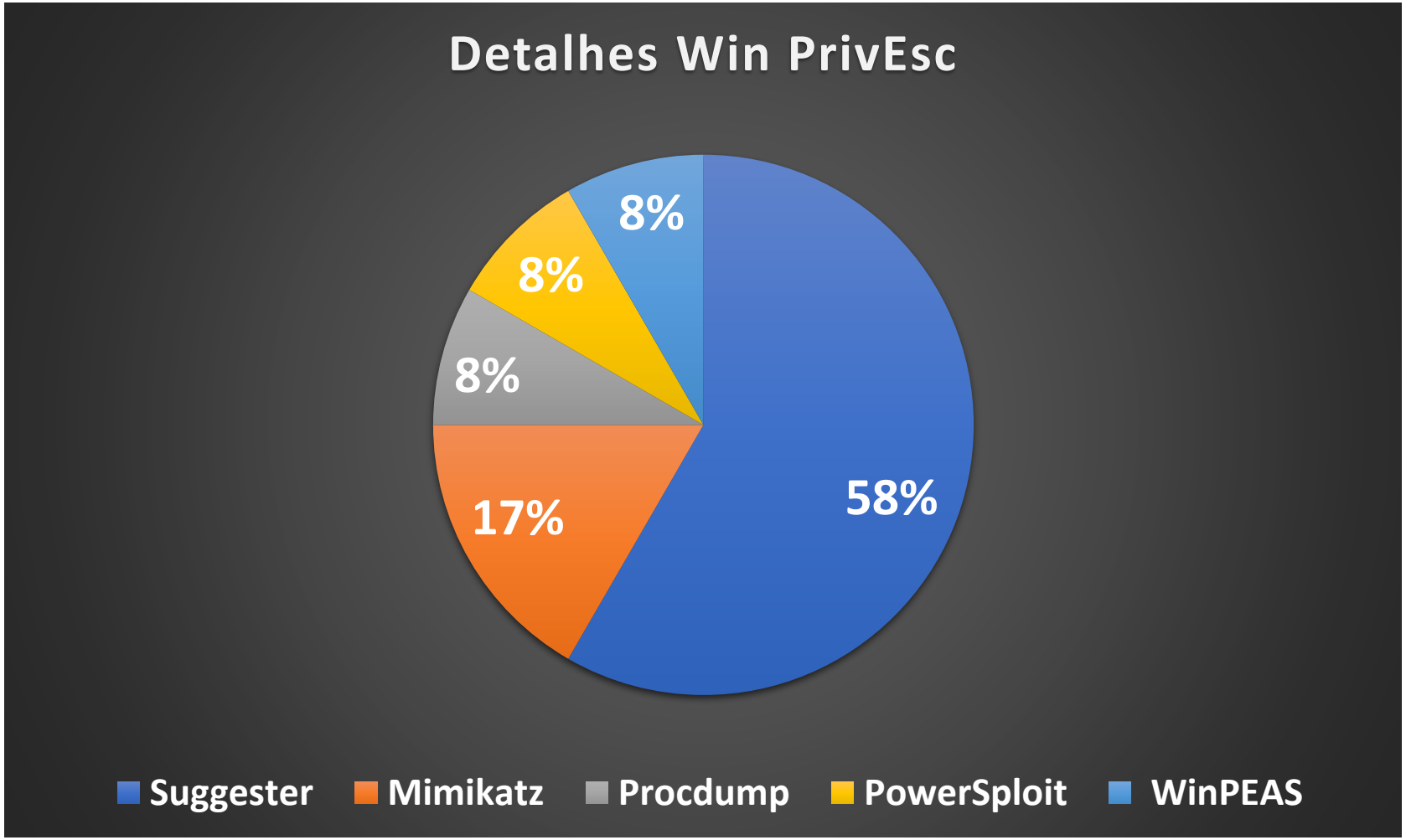


Hack The Box – Pos Exploração Windows



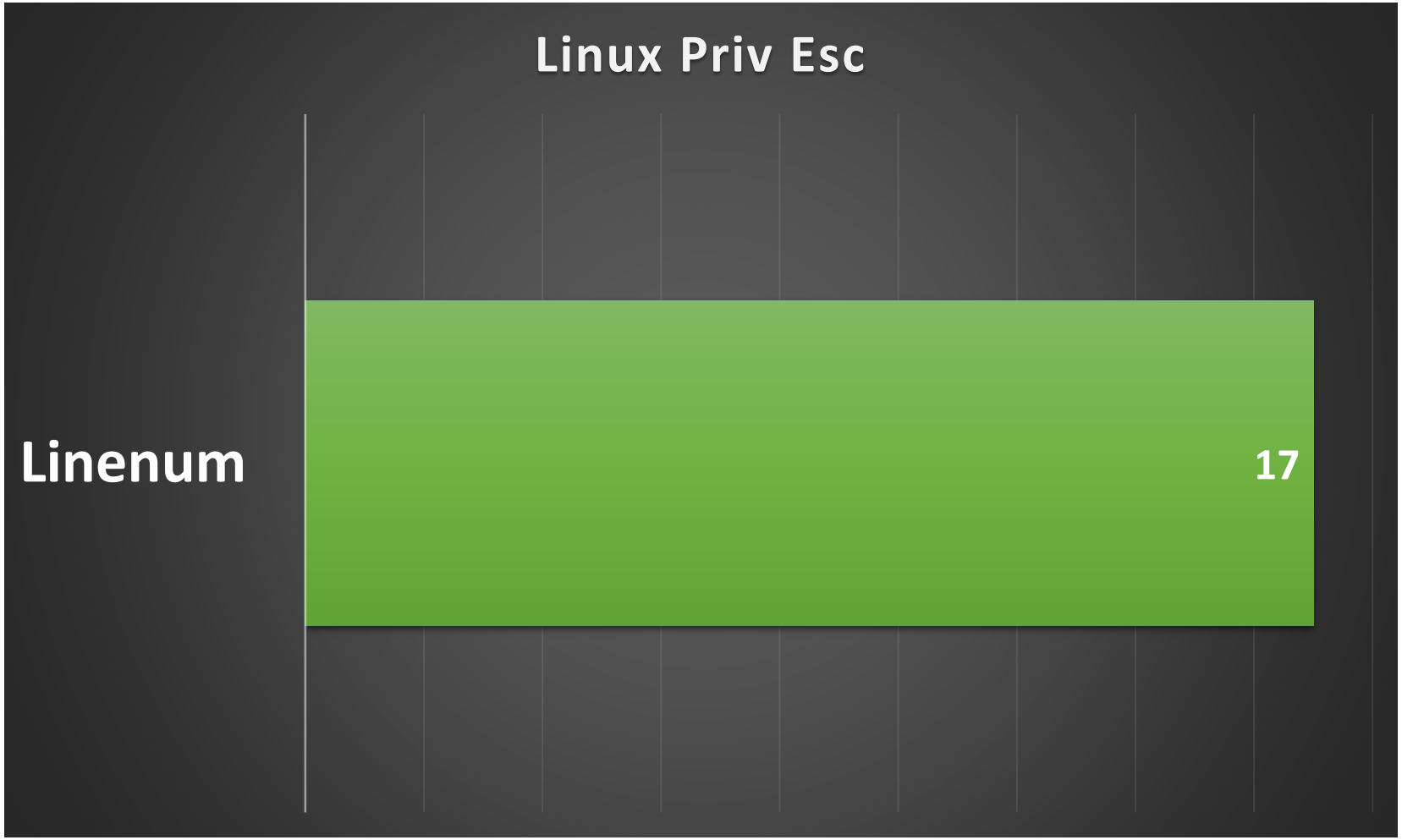
*Considerando apenas a amostra de maquinas que são Windows

Hack The Box – Pos Exploração Windows



*Considerando apenas a amostra de maquinas que são Windows

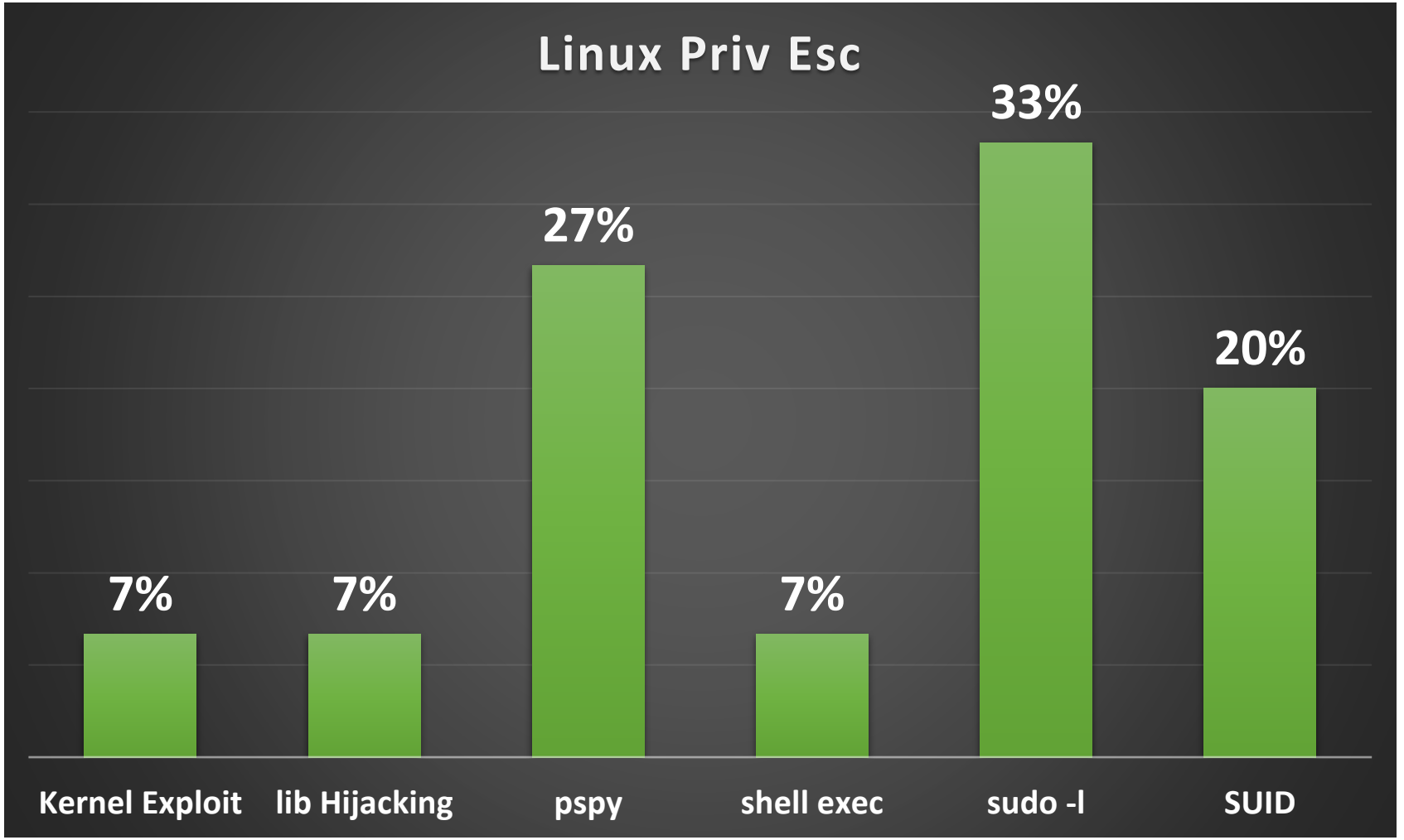
Hack The Box – Pos Exploração Linux



De 17 Maquinas Linux que necessitavam de Priv Esc para Root nas 17 foi utilizado o Linenum.

***Considerando apenas a amostra de maquinas que são Linux**

Hack The Box – Pos Exploração Linux



***Considerando apenas a amostra de maquinas que são Linux**

O que aprendemos...

Automatizando...

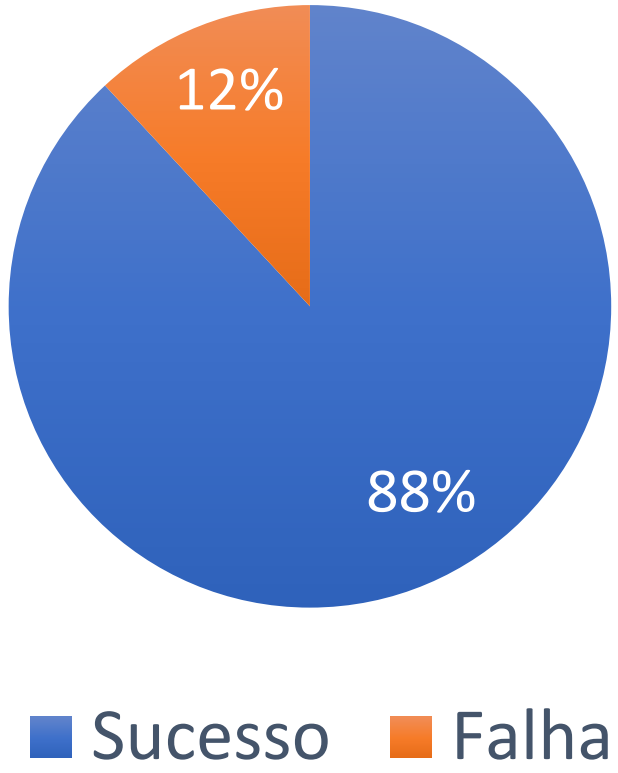
#Enumeração
nmap -A -v <IP>

#BruteForce WEB
Dirbuster

#Opções de Exploração
Metasploit
Exploits Públicos

#Windows Priv Esc
Suggester

#Linux Priv Esc
Linenum



Melhorando o que temos hoje...

Enumeração

Nmap

nmap -sT -T2 –n -Pn -p- -vv -oA <itemname> 10.10.10.10

-sT (Utilização de –sS naturamente infica Scan)
-T2 (Documentação do Nmap nos coloca e –T0 e T1 nao evitão alertas de IDS)
-Pn (Desativa os teste de descoberta padrão do Nmap)
-n (Sem resolução de DNS)
-oA (Arquivo de saida)

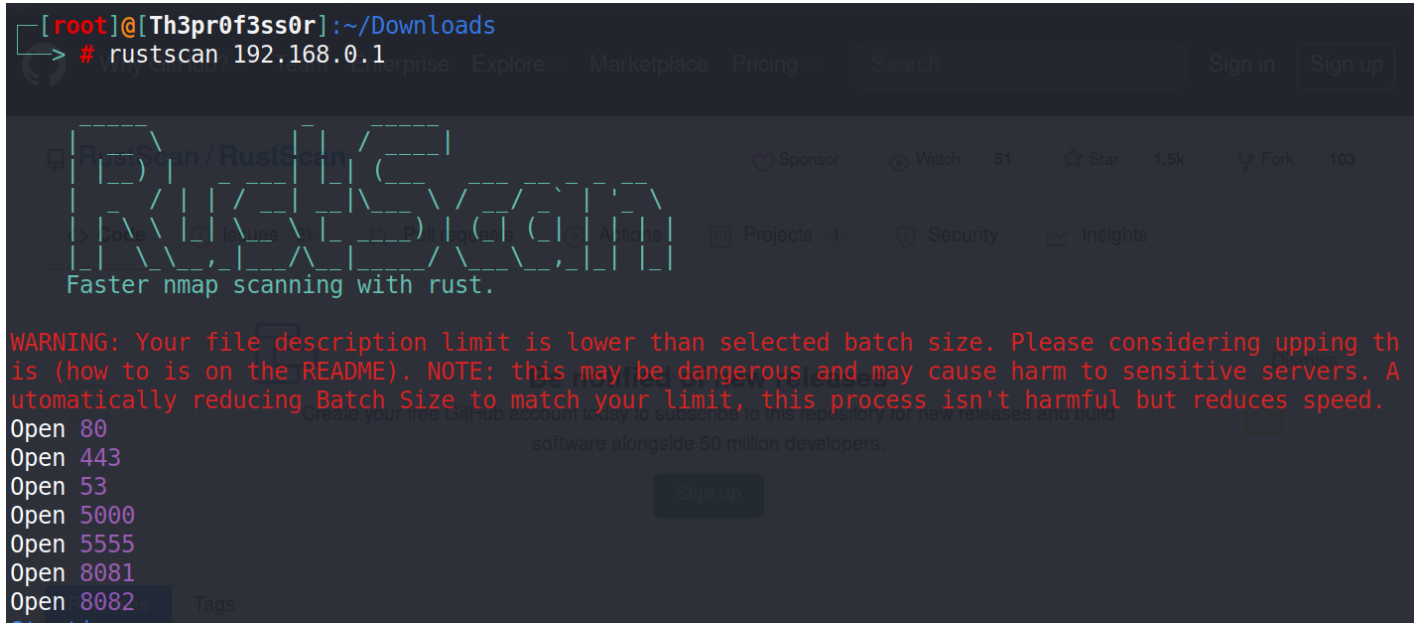
Automatizando...

Enumeração

RustScan

Transforma uma verificação Nmap de 17 minutos em 19 segundos.

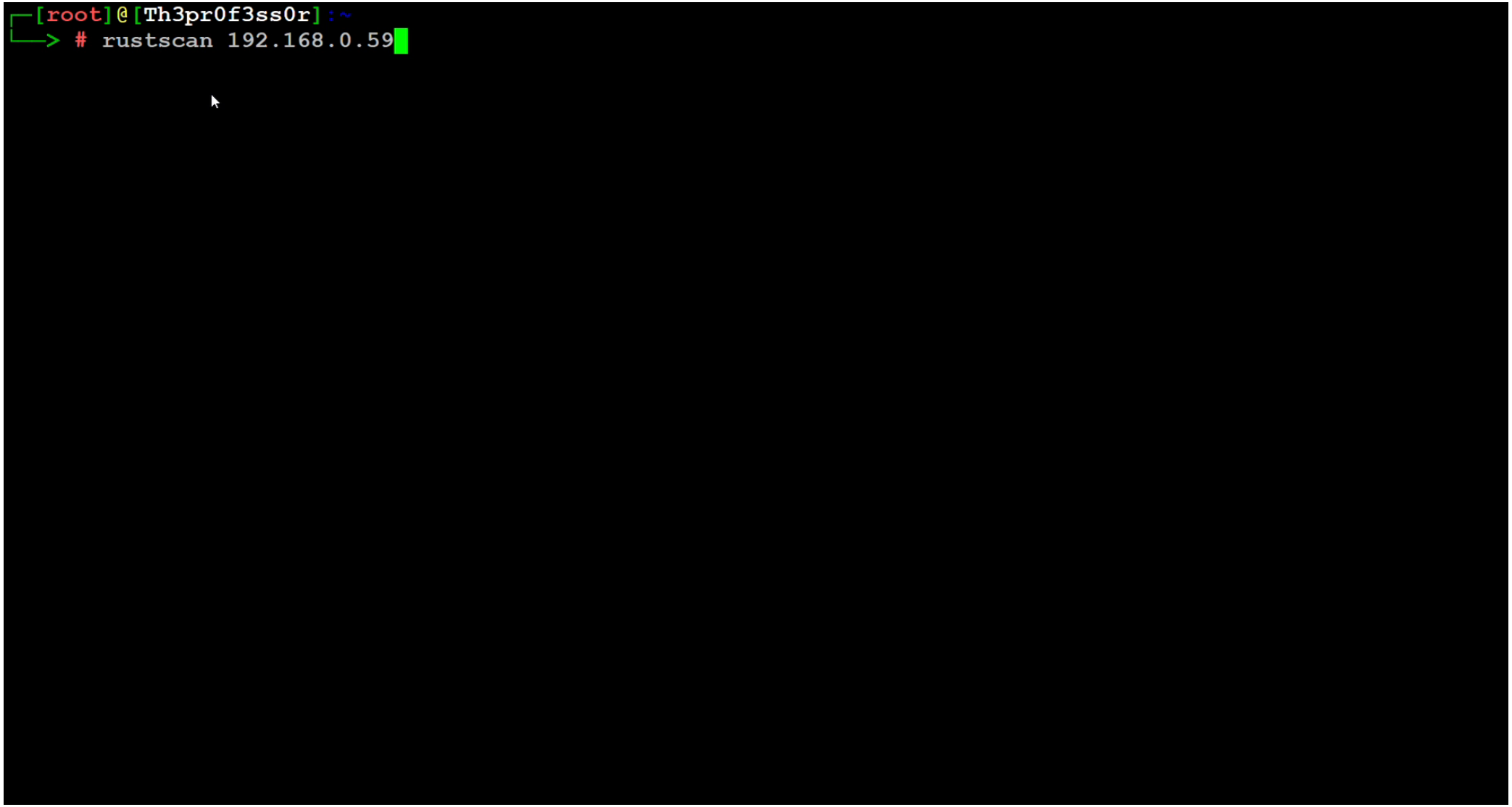
```
#  dpkg -i rustscan_1.4.0_amd64.deb
```



DEMO

RustScan

RustScan



Melhorando o que temos hoje...

Exploração

Metasploit

```
# msfconsole
spool /root/pentesname.log
setg ConsoleLogging true
setg verbose true
setg LogLevel 5
setg SessionLogging true
setg TimestampOutput true
setg PromptTimeFormat %Y%m%d.%H%M%S%z
setg PROMPT %T S:%S J:%J
setg ExitOnSession false
setg DisableCourtesyShell true
```

Ativação de Logs automatiza o tempo e evitar perda de informações importantes

Automatizando...

Exploração

Jok3r

Network & Web Pentest Automation Framework

```
root@jok3r-docker:~/jok3r# python3 jok3r.py attack -t https://192.168.0.1/ --add2db defcon

                    `-:/++++/:-.    .-:/++++/:-`
                .:ohdddmmmmdd.\  /.dddmmmmdddho:.
              `:ydmmmmmmmmmmmmm\/mmmmmmmmmmmmmmmdy:`
            `+dmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmd+`
          +dyo+++oshmmmmmmmmmmmmmmmmmmmmmmmmmmhso+++oyd+
        -+-         .dmmmmmmmmmmmmmmmmmmmmmmd.         -+-
      ``            `dmmmmmmmmmmmmmmmmmmmmmmd`            ``
                    `dmmmmmmmmmmmmmmmmmmmmmmd`
                    `ymmmmmmmmmmmmmmmmmmmmmmy`
                      .+dmmmmmmmmmmmmmmmmd+.
                         /dmmmmmmmmd/
                           `odmmdo`
                             .hh.

                                                v3.0 beta 2

                [ Network & Web Pentest Automation Framework ]

[*] URL given as target, targeted service is HTTP
[*] Reverse DNS lookup for 192.168.0.1...
[*] No DNS name found for IP
[*] Check if service is reachable...
[*] Grab service info for [host 192.168.0.1 | port 443/tcp | service http] via Nmap...
```

Jok3r

sudo docker pull koutto/jok3r

sudo docker run -i -t --name jok3r-container -w /root/jok3r -e DISPLAY=$DISPLAY -v /tmp/.X11-unix:/tmp/.X11-unix --shm-size 2g --net=host koutto/jok3r

Joker

python3 jok3r.py db

jok3rdb[default]> mission -a defcon
[+] Mission "defcon" successfully added
[*] Selected mission is now mayhem
jok3rdb[mayhem]>

python3 jok3r.py attack -t https://192.168.0.1/ --add2db defcon

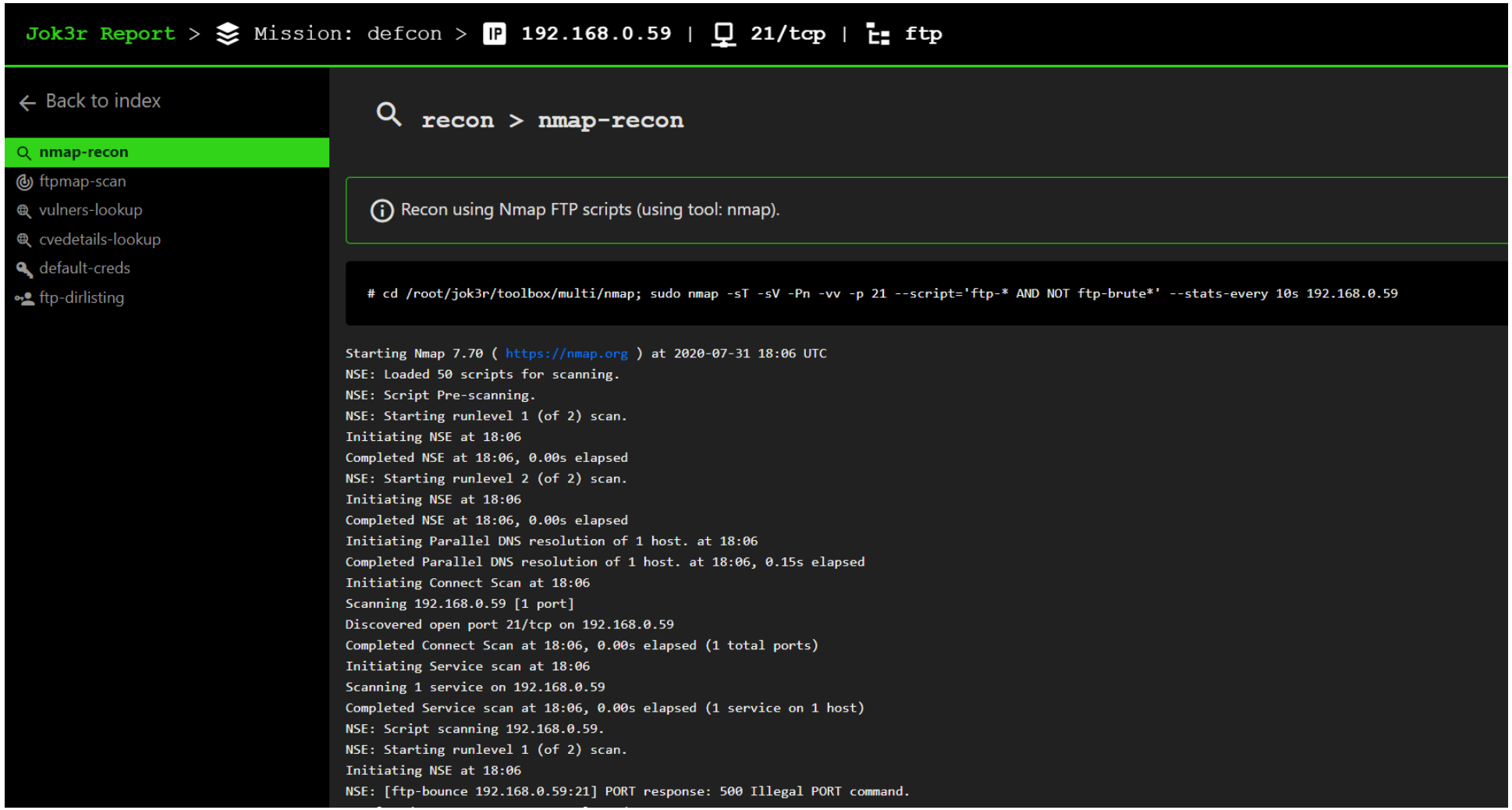
python3 jok3r.py attack -t 192.168.0.59 -s ftp --add2db defcon

Jok3r


```
jok3rdb[defcon]> report

[*] Taking web page screenshots for HTTP services (total: 2)...
[*] [1/2] Taking screenshot for https://192.168.0.1...
[*] [2/2] Taking screenshot for http://192.168.0.59...
[*] index.html file generated
[*] results-192.168.0.59-80-http-2.html file generated
[*] results-192.168.0.59-21-ftp-3.html file generated
[+] HTML Report written with success in: /root/jok3r/reports/defcon-20200731181212
[*] Important: If running from Docker container, make sure to run "xhost +" on the host before
[?] Would you like to open the report now ? [Y/n] n
```

Jok3r


Jok3r Report > Mission: defcon > IP 192.168.0.59 | 21/tcp | ftp
Back to index
nmap-recon
ftpmap-scan
vulners-lookup
cvedetails-lookup
default-creds
ftp-dirlisting
recon > nmap-recon
Recon using Nmap FTP scripts (using tool: nmap).
cd /root/jok3r/toolbox/multi/nmap; sudo nmap -sT -sV -Pn -vv -p 21 --script='ftp-* AND NOT ftp-brute*' --stats-every 10s 192.168.0.59
Starting Nmap 7.70 (https://nmap.org) at 2020-07-31 18:06 UTC
NSE: Loaded 50 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 18:06
Completed NSE at 18:06, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 18:06
Completed NSE at 18:06, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 18:06
Completed Parallel DNS resolution of 1 host. at 18:06, 0.15s elapsed
Initiating Connect Scan at 18:06
Scanning 192.168.0.59 [1 port]
Discovered open port 21/tcp on 192.168.0.59
Completed Connect Scan at 18:06, 0.00s elapsed (1 total ports)
Initiating Service scan at 18:06
Scanning 1 service on 192.168.0.59
Completed Service scan at 18:06, 0.00s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.0.59.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 18:06
NSE: [ftp-bounce 192.168.0.59:21] PORT response: 500 Illegal PORT command.

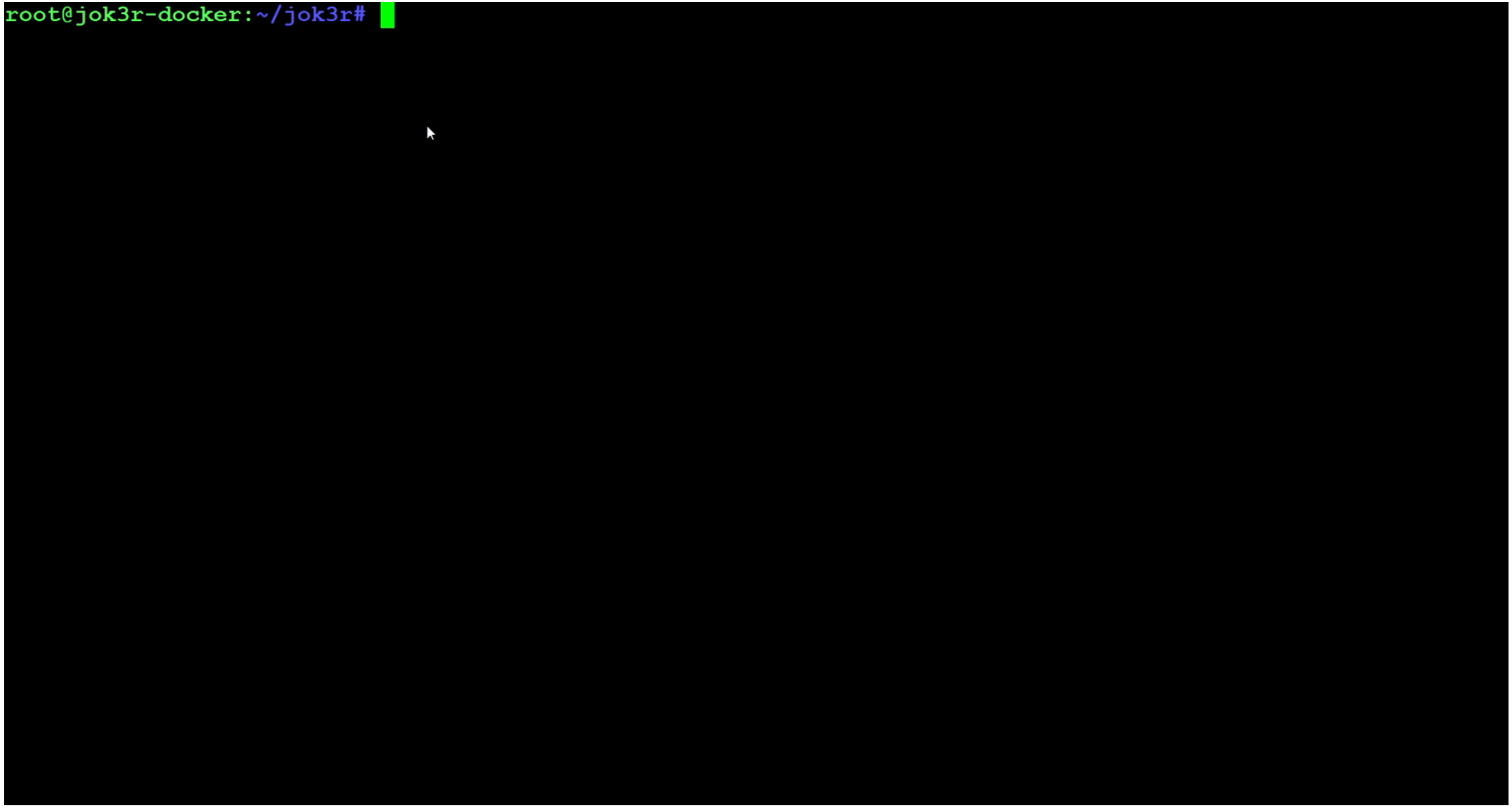
DEMO

Jok3r

Joker


root@jok3r-docker:~/jok3r# python3 jok3r.py attack -t 192.168.0.59 -s ftp --add2db defcon

Joker

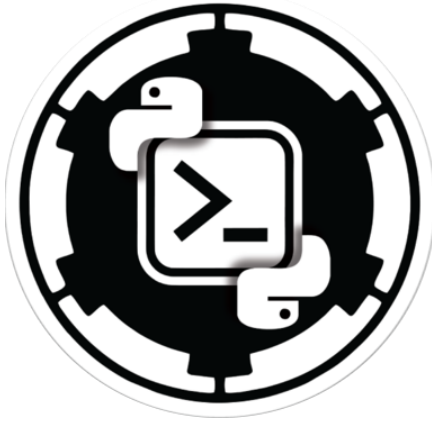


Automatizando...

Pôs Exploração e Itens para Relatório

Utilização de C2

- Empire
- Covenant
- Silent Trinity
- Faction



Guardando as informações

apt-get install sshfs

//repository/pentest_name/0-admin
//repository/pentest_name/1-recon
//repository/pentest_name/2-enumeration
//repository/pentest_name/3-targets
//repository/pentest_name/4-payload
//repository/pentest_name/5-screenshots
//repository/pentest_name/6-logs

Guardando as informações

Formato

- Screenshot Nmap port 21

20200108_1412_192.168.57.111_nmap21.png

- Screenshot of password file

20200108_1412_192.168.57.111_ftp_passwords.txt

Referencias

- Physical Red Team Operations: Physical Penetration Testing
- Hands-On Penetration Testing with Python
- Red Team Development and Operations: A practical guide
- https://hackthebox.eu
- https://github.com/koutto/jok3r
- https://github.com/RustScan/RustScan

Hacking de Planet by RH

Thank you! ☺

rafael.santos@fiap.com.br